REMARKS

Reconsideration of the pending application is respectfully requested on the basis of the following particulars:

Examiner interview

Applicant appreciates the courtesy extended to Applicant's representative during the personal interview conducted on March 19, 2008. During the interview, claim 1 was discussed in view, primarily, of the Buffam reference. In particular, Applicant's representative pointed out that Buffam uses "False Image Points" (FIPs), and not data representing an actual biometric feature, for generation of an encryption key.

It was agreed that clarification of the biometric feature and how the encrypted code word would overcome the prior art of record.

In the claims

Claim 1 has been amended to more clearly refer to the biometric feature, and to define how the encrypted code word is generated.

In particular, claim 1 is amended to point out that the encrypted code word is formed by digitizing a biometric feature to create a digital representation of the biometric feature, fault-tolerantly encoding the secret data to create a code word, and encrypting the code word on the basis of the digital representation of the biometric feature. Support for this amendment is found at least at page 13 of the original specification, and in original claims 2 and 3.

Claims 2 and 20 are amended to more clearly refer to the biometric feature, in a manner generally corresponding to the amended claim 1.

Rejection of claims 1-3, 5-7, and 10-26 under 35 U.S.C. § 103(a)

Claims 1-3, 5-7, and 10-26 presently stand rejected as being unpatentable over Buffam (U.S. 6,185,316) in view of Matyas et al. (U.S. 6,697,947). This rejection is respectfully traversed for at least the following reasons.

It is respectfully submitted that neither Buffam nor Matyas disclose or suggest the presently claimed invention wherein a digital representation of the biometric feature is used, as in the present invention, for decrypting or encrypting a secret data.

While Buffam discloses an authentication apparatus and method that employs a fingerprint reader and comparison, Buffam does not use a digital representation of the fingerprint to encrypt a fault-tolerantly encoded secret data on the basis of a digital representation of a biometric feature.

Buffam instead uses "false image points" or FIPs which are generated as highly random data (see *Buffam*; col. 13, lines 63-66 and col. 20, lines 6-8). While Buffam's method selects certain of these generated FIPs as "plausible imposters" of "true image points" that correspond to a fingerprint, they are different from the fingerprint data and are derived from "highly random data" which is generated by a FIPs generator, and are not actual fingerprint data. More particularly, these FIGs. do not constitute a digital representation of a biometric feature.

Instead of using a digitized biometric authentication feature data to obtain a decrypted code word, Buffam generates ***false minutia*** (not actual biometric data). According to Buffam, "the false minutiae (FIPs) can be hashed to form an encryption key, step 725." (*Buffam*; col. 20, lines 55-56). The false minutiae (FIPs) are included with (but are not) ***true minutia*** that correspond to a user's fingerprint pattern to form a "transient template" which is stored on a user's credential.

In practice, a claimant "presents credential 605 to credential sensor 615 contemporaneously with providing a live fingerprint scan from fingerprint sensor 614. Thransient template 620 is then extracted from credential 605. From template 620 is extracted candidate [false minutia] vector 635." (*Buffam*; col. 20, line 66 – col. 21, line 3).

The user's live fingerprint scan is compared to the ***true minutia*** (TIPs). "If claimant 612 is the same person as represented by the data encoded into credential 605, as determined in comparator 650, the fingerprint scan [***true minutia***] TIPs read in sensor 614 will correspond with the proffered [***true minutia***] TIPs vector from credential 605." (*Buffam*; col. 21, lines 4-8).

After the ***true minutia*** are extracted, "there will remain the set of [***false minutia***] FIPs data 635, which can be hashed in decode key generator 640 to produce decode key 645.

Thus, the decode key 645 is not based on any user biometric data, but is based on the ***false minutia*** which are entirely "made up" data not derived from the actual user biometric data (TIPS or ***true minutia***) at all. Instead, the false minutia are "false image points (FIP) 128 [which] can be created by FIP generator (FIPG) 130, with the FIPs 128 preferably having a substantial degree of entropy, i.e., having a ***highly random content***." (*Buffam*; col. 13, lines 63-66).

Therefore, Buffam does not teach or suggest that an encrypted code word is decrypted on the basis of a digitized biometric feature data, thereby obtaining a decrypted code word. More particularly, Buffam does not teach or suggest that an encrypted code word is decrypted on the basis of a digital representation of a biometric feature.

Moreover, Buffam does not disclose or suggest first fault-tolerantly encoding secret data to create a code word, and then encrypting the code word on the basis of a digital representation of the biometric feature as in the present invention.

Matyas, in contrast with both Buffam and the present invention, discloses a method to combine biometric features of a plurality of uses, and to authenticate only when the biometric features of a sufficient number of users have been recognized. (see *Matyas*; col. 9, lines 11-14, 24-28).

Thus, Matyas differs from the present invention in that, according to Matyas, authentication is carried out only after the biometric features of a sufficient number of users have been recognized.

Matyas does not disclose or suggest that a secret data is recovered from a decrypted code word on the basis of a coding theory method within a freely selectable tolerance interval.

More particularly, Matyas does not disclose or suggest using a biometric feature to decrypt an encrypted code word wherein the encrypted code word is formed by digitizing a biometric feature to create a digital representation of the biometric feature, fault-tolerantly encoding the secret data to create a code word, and encrypting the code word on the basis of the digital representation of the biometric feature.

Even assuming, *arguendo*, that Matyas discloses that a secret key SK may be obtained from a user's biometric feature by decrypting an encrypted code word on the basis of the biometric authentication feature, and recovering secret data from the decrypted code word on the basis of a coding-theory method within a freely selectable tolerance window, it must be appreciated that Buffam's decode key is contained in the ***false minutia***, and is therefore not at all related to a user's biometric feature represented by the true minutia.

Since Buffam's true minutia are unrelated to Buffam's decode key, applying Matyas' teachings to Buffam's user biometric data (represented by the true minutia) will not result in extracting the decode key. On the other hand, applying any teachings of Matyas to Buffam's false minutia would not result in secret data obtained by decrypting an encrypted code word on the basis of a digitized biometric authentication feature, because the false minutia are not digitized biometric authentication feature but are instead essentially made-up, random data.

Further, modifying Buffam such that the decode key is extractable from the true minutia would change the principle of operation of Buffam, since Buffam is based on a principle of generating a key from false image points (FIPs, or false minutia) separate and different from actual biometric data represented as true image points (TIPs, or true minutia).

For at least these reasons, Buffam and Matyas together fail to disclose or suggest each and every element of the presently claimed invention, and therefore fail to form a prima facie case of obviousness of any of the presently pending claims. Accordingly, it is respectfully submitted that claims 1-26 are allowable over the cited references, and withdrawal of the rejection is requested.

Rejection of claims 4, 8, and 9 under 35 U.S.C. § 103(a)

Claims 4, 8, and 9 presently stand rejected as being unpatentable over Buffam and Matyas in view of Camp, Jr. et al. (U.S. 6,075,987). This rejection is respectfully traversed for at least the following reasons.

As discussed above, Buffam and Matyas fail to disclose or suggest each and every element of claim 1. It is respectfully submitted that Camp fails to supplement the deficiencies of the Buffam and Matyas, and therefore Buffam, Matyas, and Camp together fail to form a prima facie case of obviousness of claim 1, and therefore claims 4, 8, and 9 are allowable over the cited references at least due to their dependency from claim 1. Accordingly, withdrawal of the rejection is requested.

Conclusion

In view of the amendments to the claims, and in further view of the foregoing remarks, it is respectfully submitted that the application is in condition for allowance. Accordingly, it is requested that claims 1-26 be allowed and the application be passed to issue.

If any issues remain that may be resolved by a telephone or facsimile communication with the Applicant's attorney, the Examiner is invited to contact the undersigned at the numbers shown.

Respectfully submitted,

BACON & THOMAS, PLLC
625 Slaters Lane, Fourth Floor
Alexandria, Virginia 22314-1176
Phone: (703) 683-0500

Date: April 14, 2008

JOHN R. SCHAEFER
Attorney for Applicant
Registration No. 47,921